FIG. 1

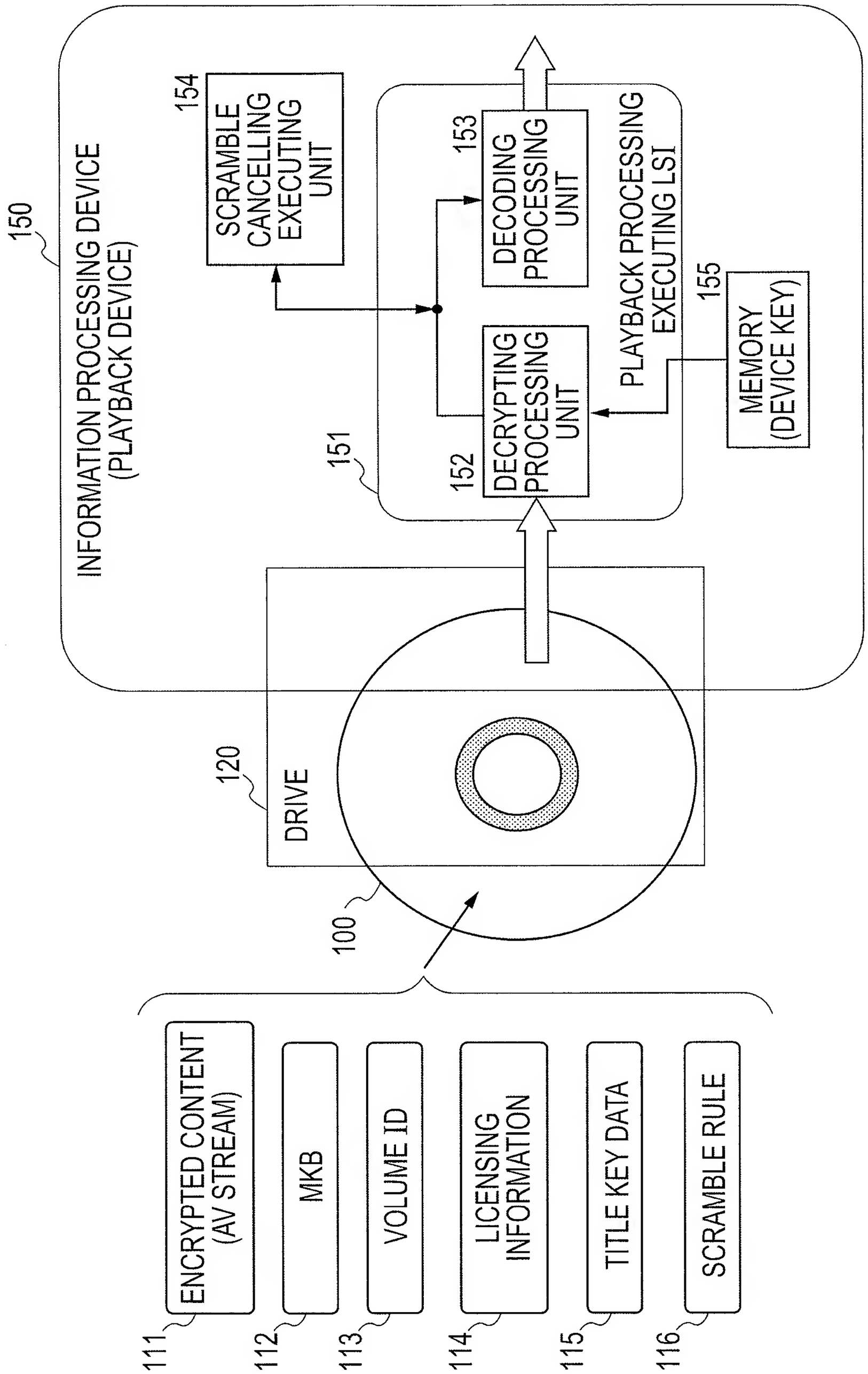

100
120
DRIVE
150
INFORMATION PROCESSING DEVICE
(PLAYBACK DEVICE)
151
152
DECRYPTING PROCESSING UNIT
153
DECODING PROCESSING UNIT
154
SCRAMBLE CANCELLING EXECUTING UNIT
PLAYBACK PROCESSING EXECUTING LSI
155
MEMORY
(DEVICE KEY)
111
ENCRYPTED CONTENT (AV STREAM)
112
MKB
113
VOLUME ID
114
LICENSING INFORMATION
115
TITLE KEY DATA
116
SCRAMBLE RULE

FIG. 2

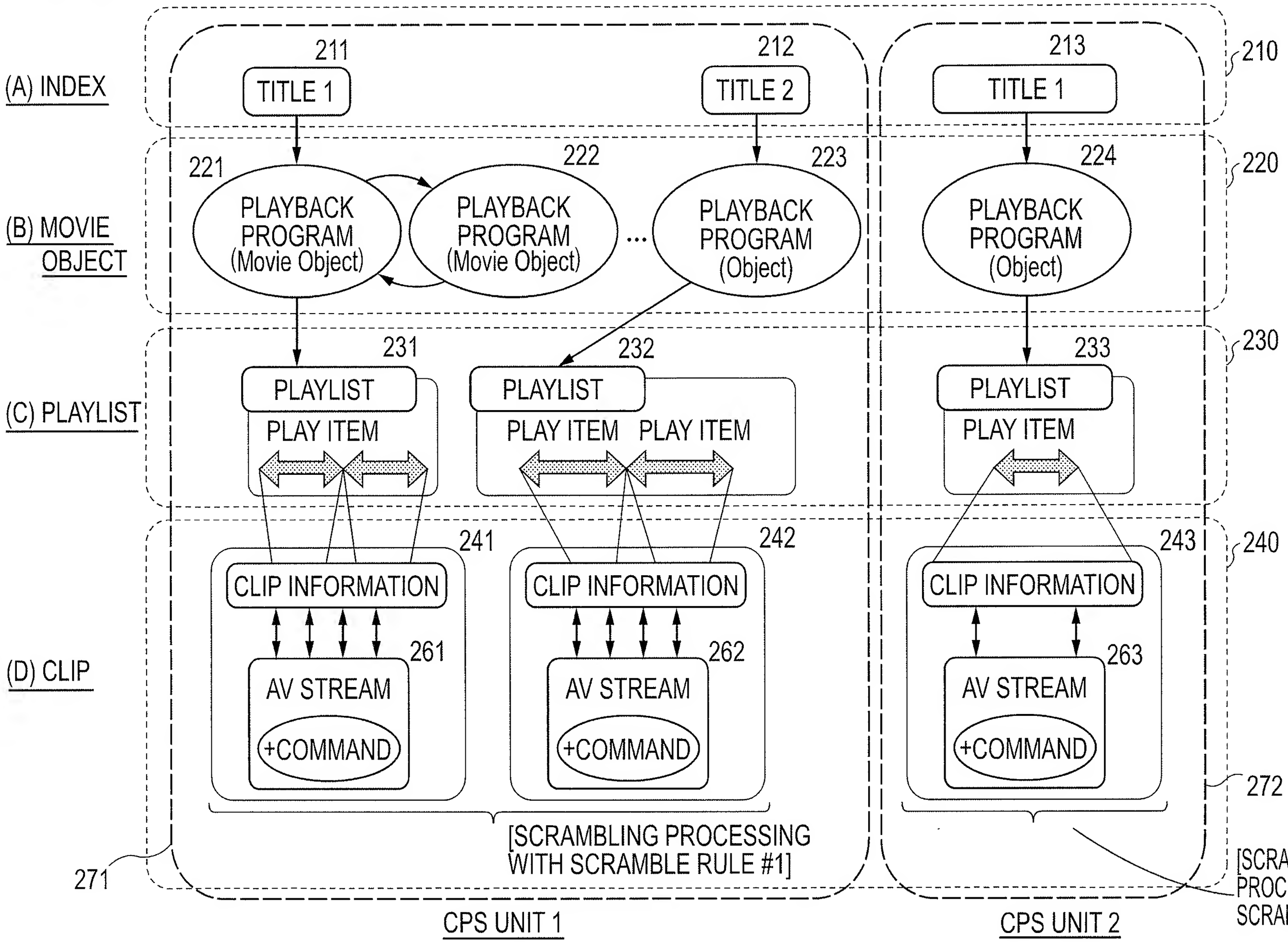


FIG. 3

INDEX DISTINGUISHABLE BY APPLICATION LAYERS SUCH AS TITLE	CONTENT MANAGEMENT UNIT (CPS)	SCRAMBLE RULE
TITLE 1	CPS1	Scr#1
TITLE 2	CPS1	Scr#1
APPLICATION 1	CPS2	Scr#2
APPLICATION 2	CPS3	Scr#3
:	:	:
DATA GROUP 1	CPS4	Scr#4
DATA GROUP 2	CPS5	Scr#5
:	:	:

FIG. 4

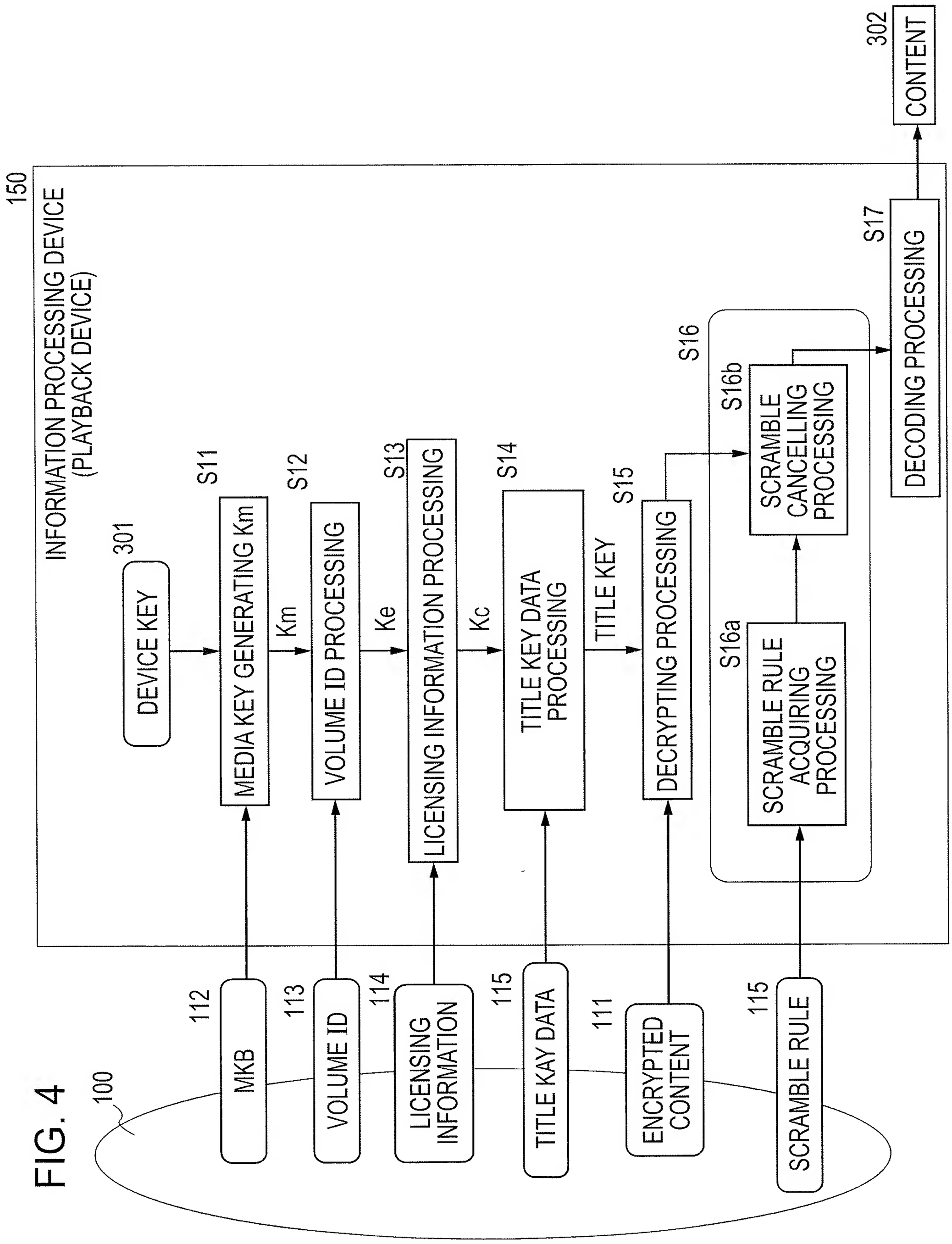
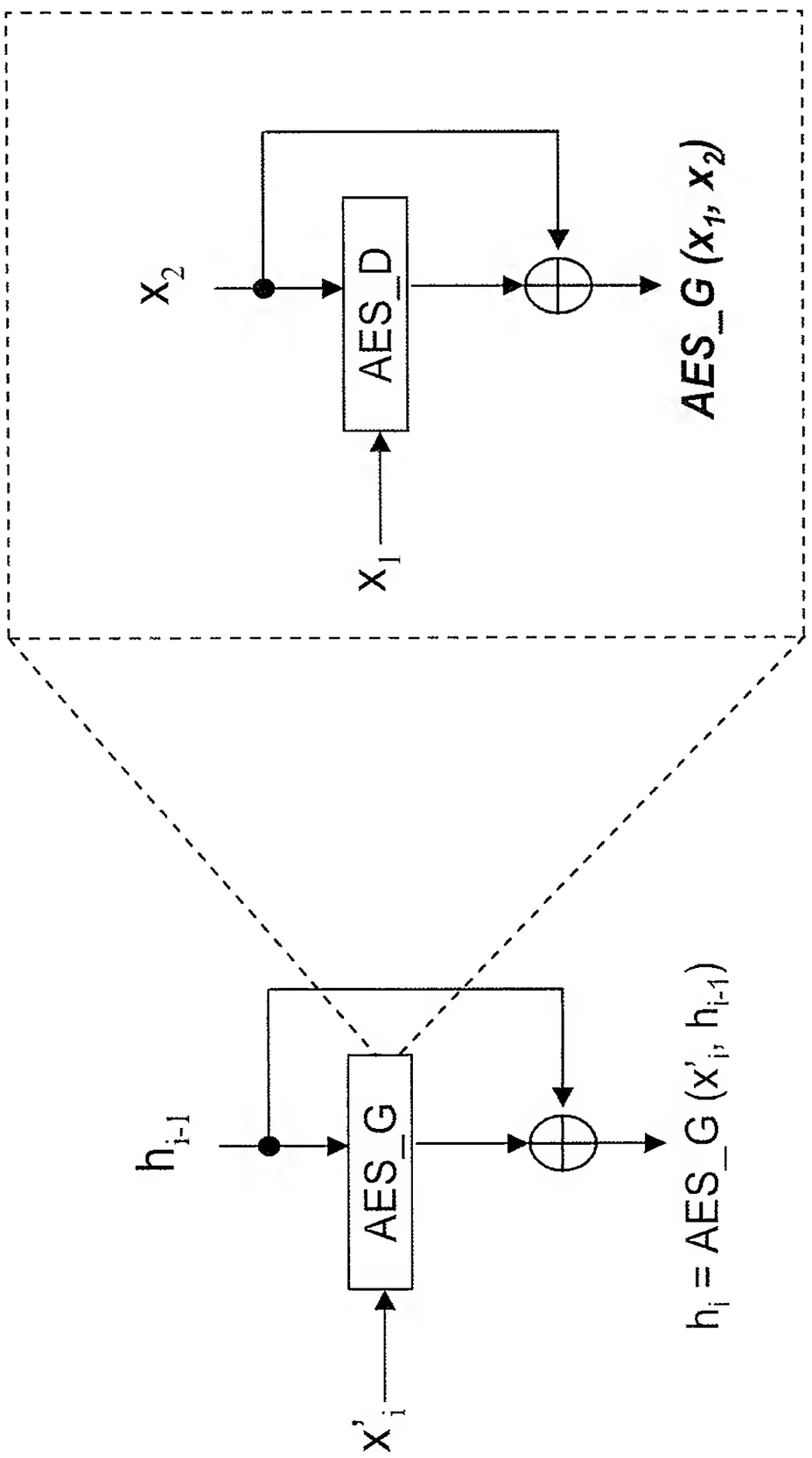

100
150
INFORMATION PROCESSING DEVICE
(PLAYBACK DEVICE)
301
DEVICE KEY
S11
MEDIA KEY GENERATING Km
Km
S12
VOLUME ID PROCESSING
Ke
S13
LICENSING INFORMATION PROCESSING
Kc
S14
TITLE KEY DATA PROCESSING
TITLE KEY
S15
DECRYPTING PROCESSING
S16
S16a
SCRAMBLE RULE ACQUIRING PROCESSING
S16b
SCRAMBLE CANCELLING PROCESSING
S17
DECODING PROCESSING
302
CONTENT
112
MKB
113
VOLUME ID
114
LICENSING INFORMATION
115
TITLE KAY DATA
111
ENCRYPTED CONTENT
115
SCRAMBLE RULE

FIG. 5



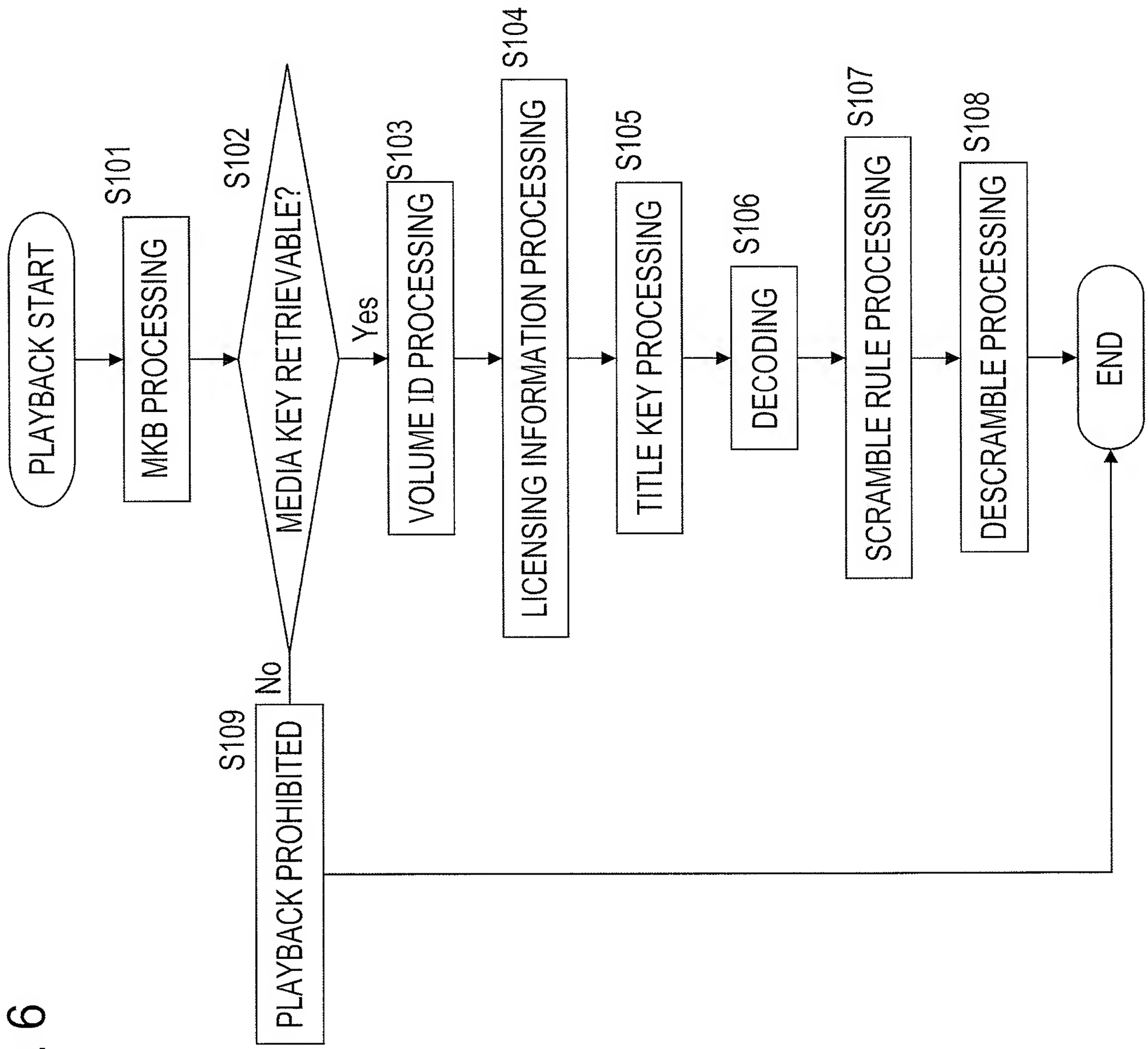

104
PLAYBACK START
S101
MKB PROCESSING
S102
MEDIA KEY RETRIEVABLE?
Yes
No
S103
VOLUME ID PROCESSING
LICENSING INFORMATION PROCESSING
S105
TITLE KEY PROCESSING
S106
DECODING
S107
SCRAMBLE RULE PROCESSING
S108
DESCRAMBLE PROCESSING
END
S109
PLAYBACK PROHIBITED

FIG. 6

FIG. 7

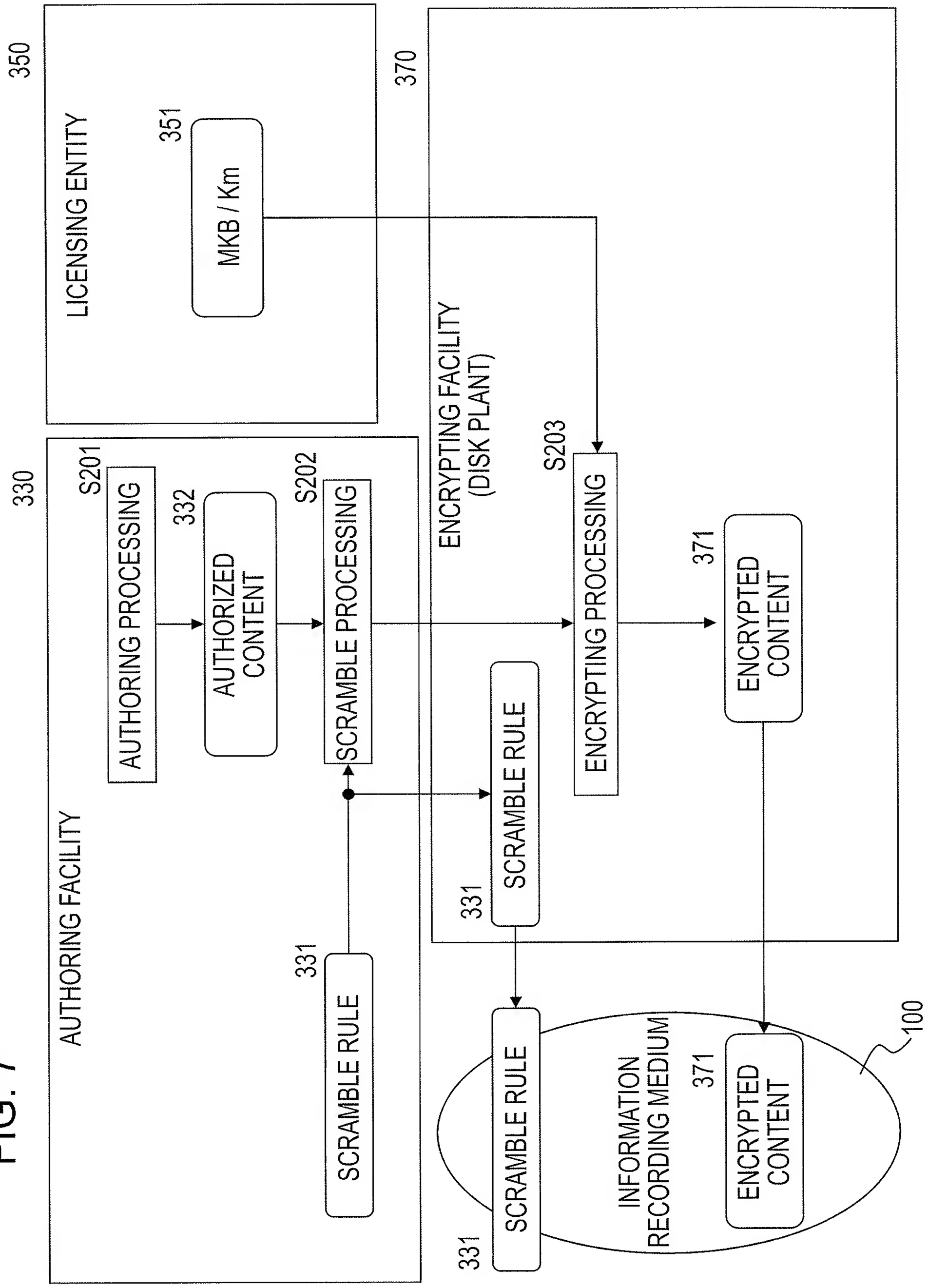

350
LICENSING ENTITY
351
MKB / Km
370
ENCRYPTING FACILITY
(DISK PLANT)
330
AUTHORING FACILITY
S201
AUTHORING PROCESSING
332
AUTHORIZED CONTENT
S202
SCRAMBLE PROCESSING
S203
ENCRYPTING PROCESSING
371
ENCRYPTED CONTENT
331
SCRAMBLE RULE
331
SCRAMBLE RULE
331
SCRAMBLE RULE
INFORMATION RECORDING MEDIUM
371
ENCRYPTED CONTENT
100

FIG. 8

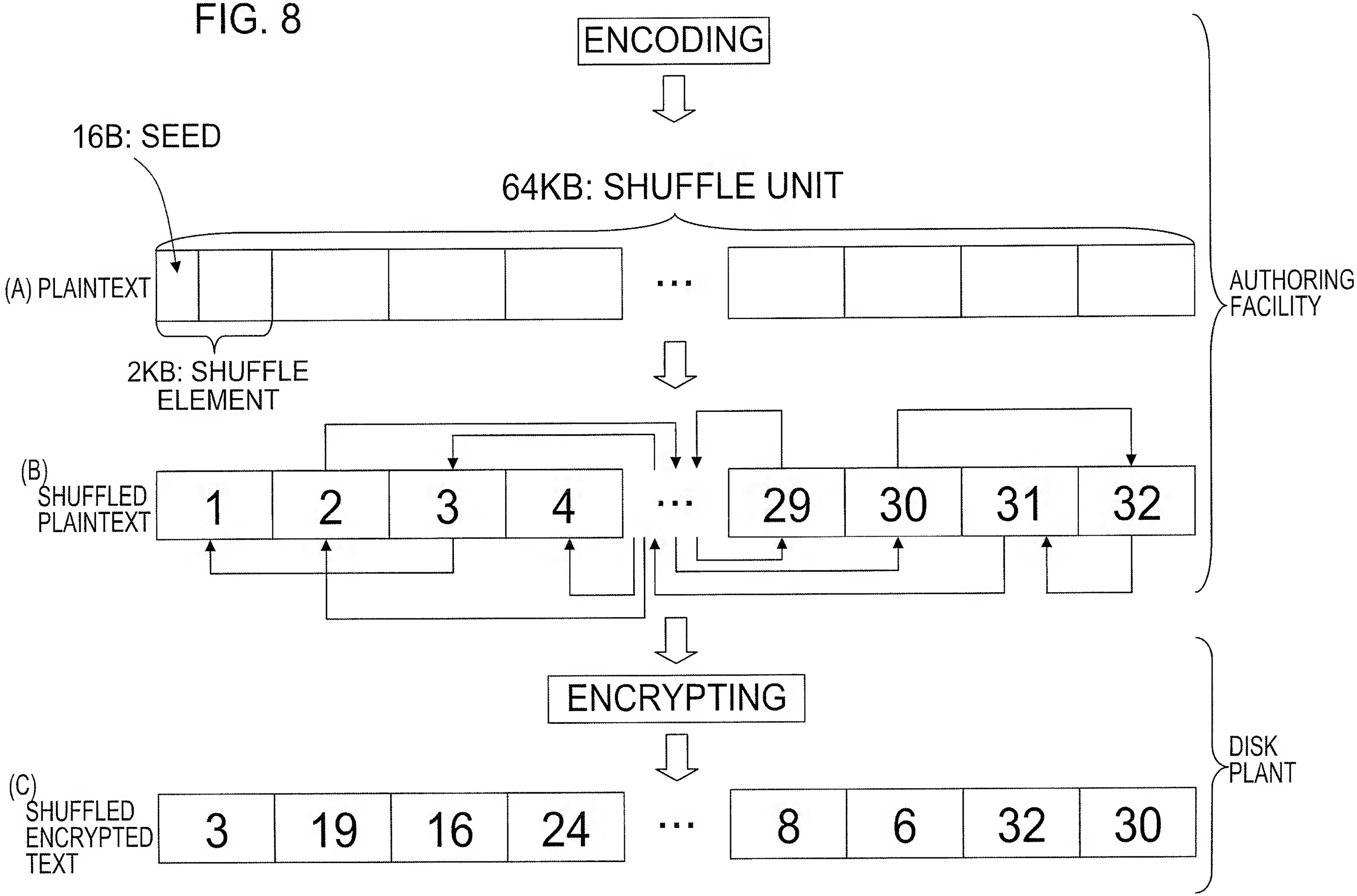

ENCODING
16B: SEED
64KB: SHUFFLE UNIT
(A) PLAINTEXT
2KB: SHUFFLE ELEMENT
AUTHORING FACILITY
(B) SHUFFLED PLAINTEXT
1
2
3
4
...
29
30
31
32
ENCRYPTING
(C) SHUFFLED ENCRYPTED TEXT
3
19
16
24
...
8
6
32
30
DISK PLANT

FIG. 9

(A) SCRAMBLE RULE (IN THE EVENT THAT THERE ARE 32 SHUFFLE ELEMENTS WITHIN THE SHUFFLE UNIT)

3	19	16	24	26	18	10	2
28	20	12	4	1	15	25	9
22	11	21	31	7	29	13	23
5	17	27	14	8	6	32	30

(B1) BEFORE SHUFFLING

1	2	3	4	5	6	7	8	9	10	11	12	.....	28	29	30	31	32

(B2) AFTER SHUFFLING

3	19	16	24	26	18	10	2	28	20	12	4	.....	14	8	6	32	30

FIG. 10

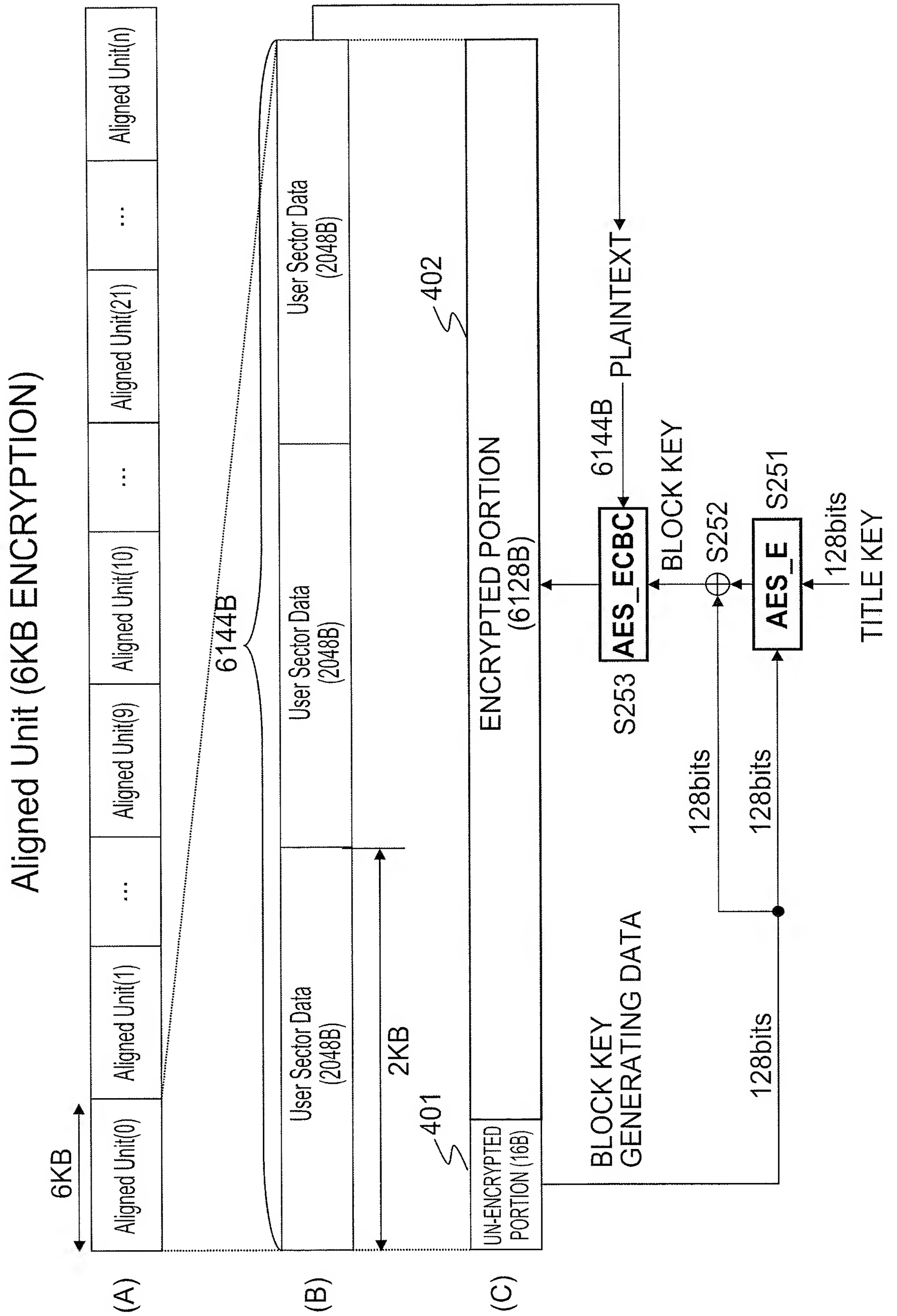
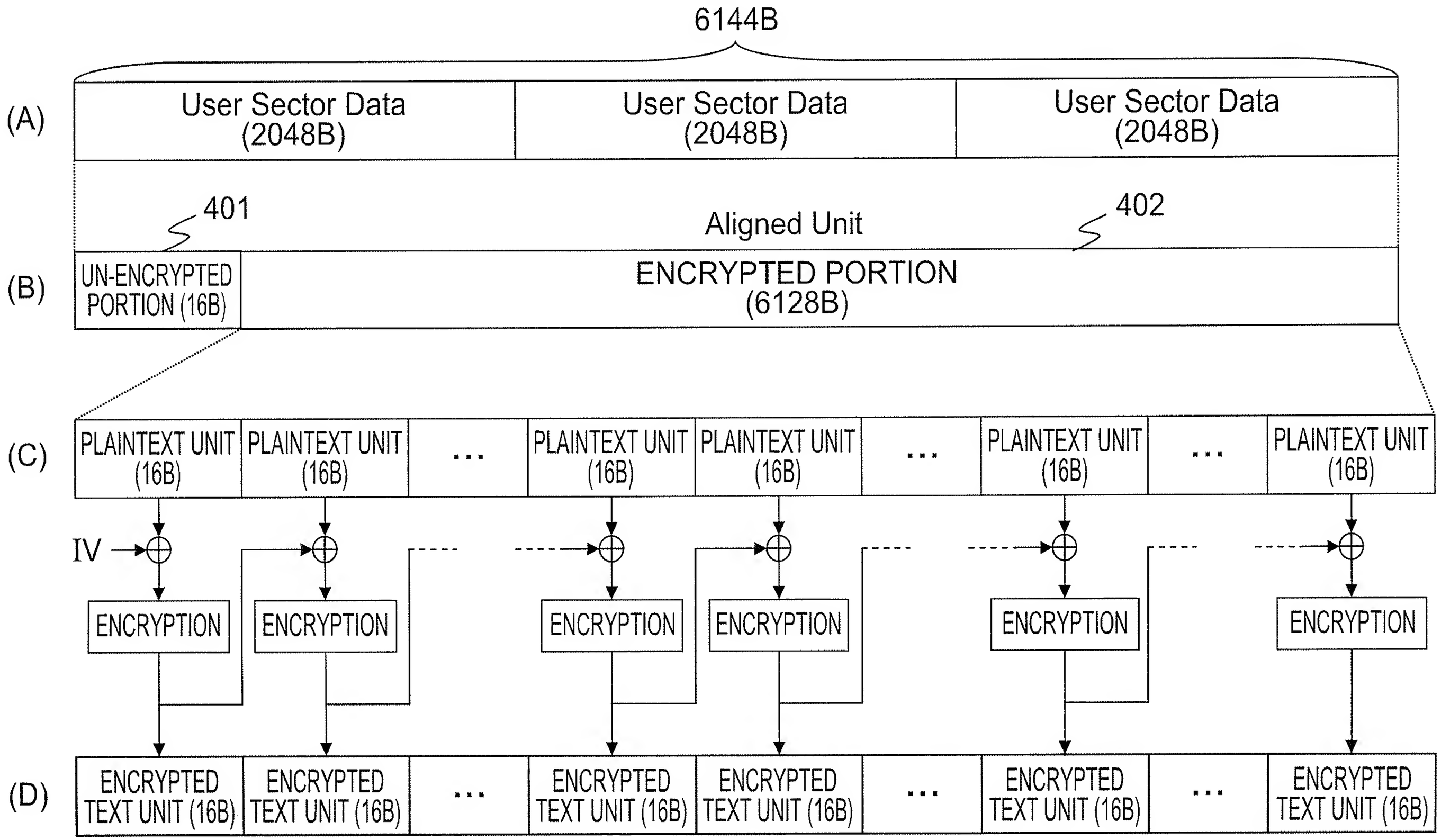

Aligned Unit (6KB ENCRYPTION)
(A)
6KB
Aligned Unit(0)
Aligned Unit(1)
...
Aligned Unit(9)
Aligned Unit(10)
...
Aligned Unit(21)
Aligned Unit(n)
(B)
6144B
User Sector Data (2048B)
User Sector Data (2048B)
2KB
401
(C)
UN-ENCRYPTED PORTION (16B)
ENCRYPTED PORTION (6128B)
402
PLAINTEXT
6144B
S253
AES_ECBC
BLOCK KEY
S252
S251
AES_E
128bits
128bits
128bits
TITLE KEY
BLOCK KEY GENERATING DATA

FIG. 11

CBC (Cipher Block Chaining) MODE (ENCRYPTED)



S05P1581

FIG. 12

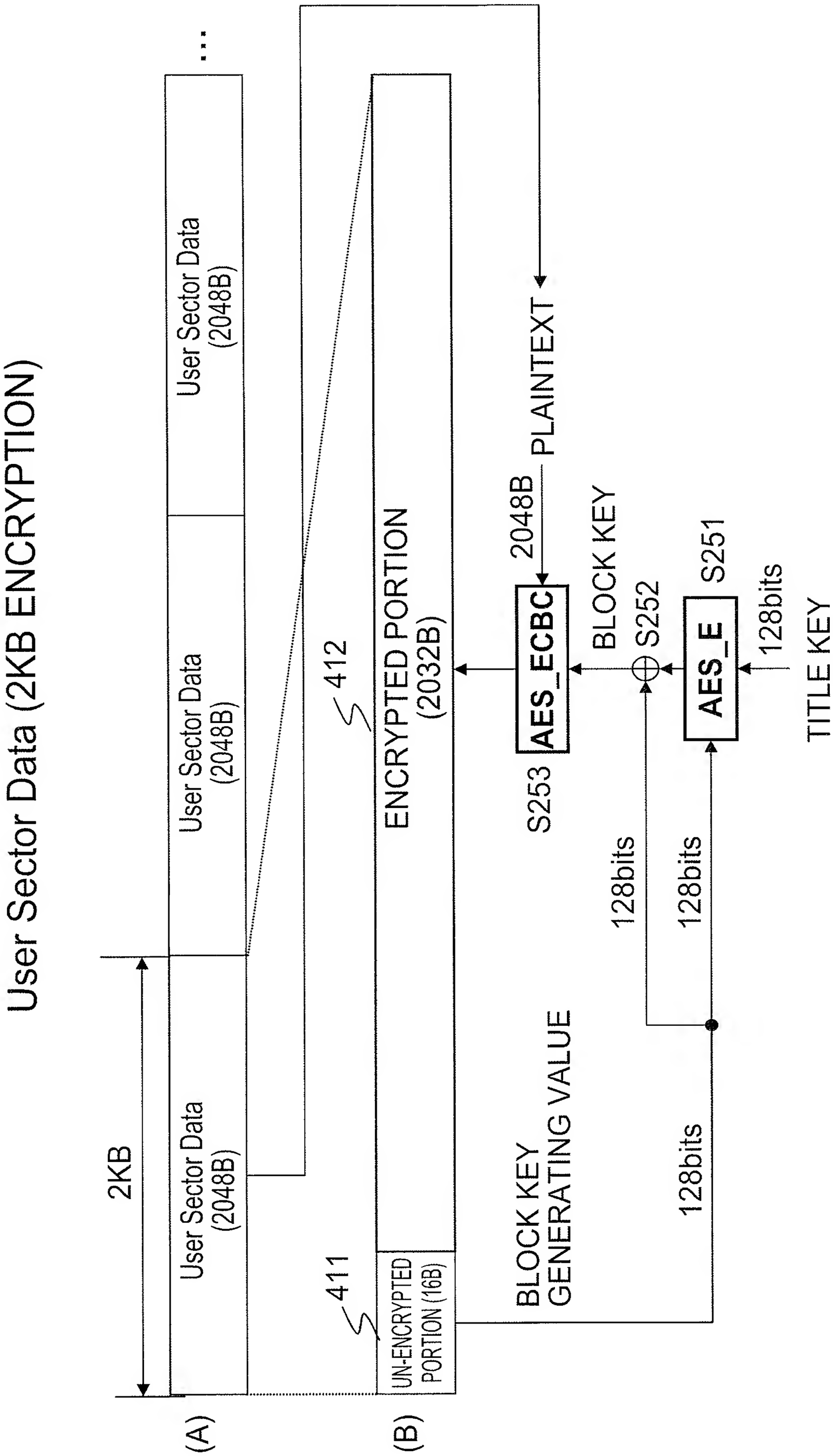


FIG. 13

MSTBL.DA (THELP FILE FOR ENCRYPTING IN DISK PLANT)

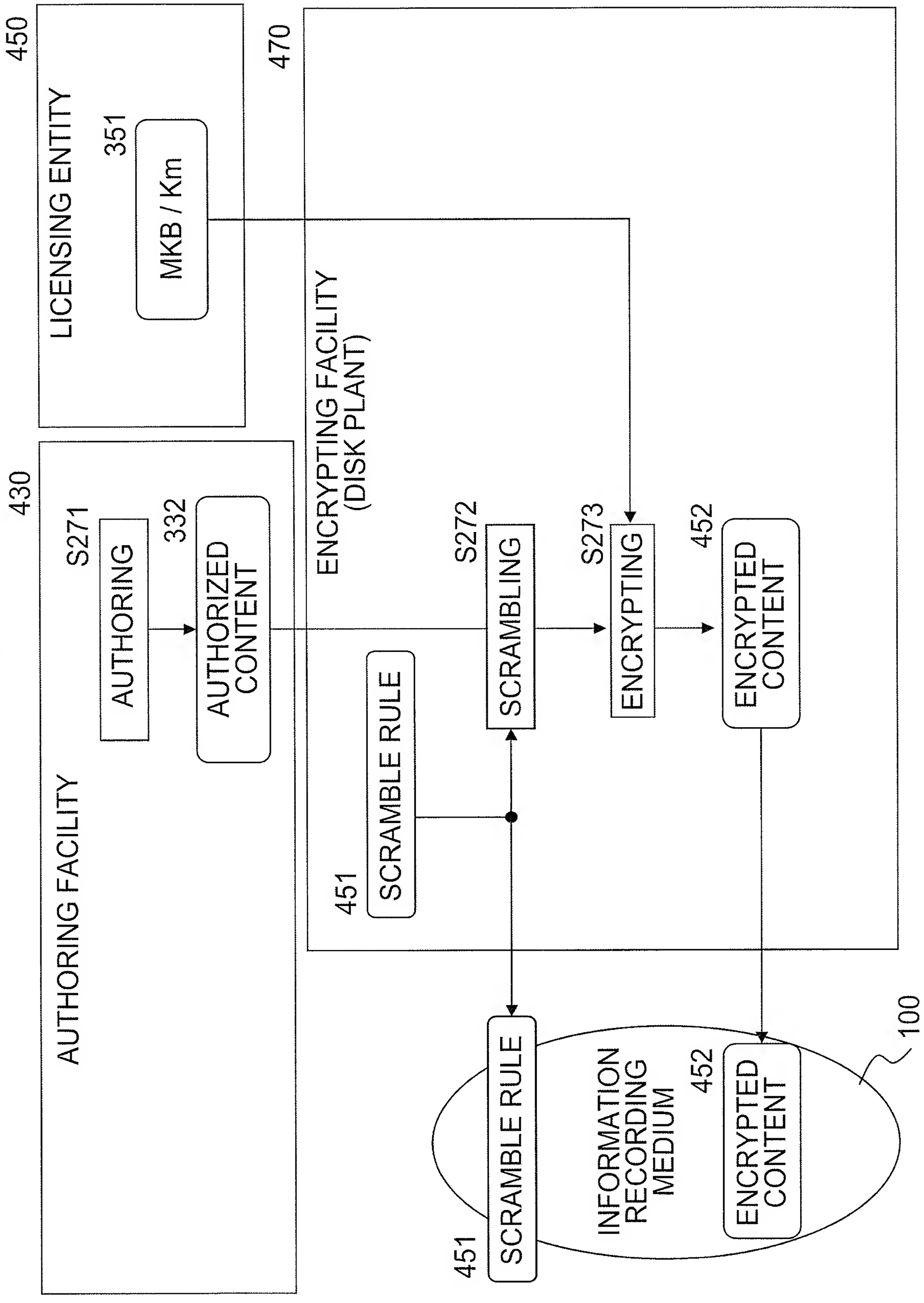
	#bits	value
Li_MSTBL.DAT( ){		
UD_START_Location	32	
UD_END_Location	32	
CHT_Location	32	
CHT_Offset	32	
Content_Cert_Location	32	
Content_Cert_Offset	32	
UK_Inf_Location	32	
UK_Inf_Offset	32	
Num_of_UK	32	
MKB_Location	32	
For (j = 1; j =<N, j++) {		
Encryption_Flag(j)	8	00_{16}: not to-be-encrypted 01_{16}: to-be-encrypted
Data_Type(j)	8	01_{16}: 1st sector of AU 02_{16}: 2nd sector of AU 03_{16}: 3rd sector of AU 04_{16}: Non-AV data (e.g. Java)
CPS_Unit_No(j)	16	0000_{16}-$FFFF_{16}$
Clip_AV_File_No(j)	24	00000-99999
Reserved	6	000000_2
Last_Sector_of_Clip(j)	1	0_2: not Last Sector of each Clip 1_2: Last Sector of each Clip
Last_Sector_of_Layer(j)	1	0_2: not Last Sector of each Clip in layer i 1_2: Last Sector of each Clip in each layer i
}		
}		

FIG. 14

SYNTAX OF MSTBL.DAT

UD_START_Location: Physical Sector Number OF START LOCATION OF User Data FOR EACH Layer (Data Zone)
UD_END_Location: Physical Sector Number OF END LOCATION OF User Data FOR EACH Layer (Data Zone)
CHT_Location: Physical Sector Number of CHT START LOCATION.
CHT_Offset: NUMBER OF BYTES UNTIL DIRECTLY BEFORE Hash Value (DATA TO BE FILLED IN BY Mastering Facility) AND START LOCATION OF CHT.
Content_Cert_Location: Physical Sector Number of Content Certificate START LOCATION.
Content_Cert_Offset: NUMBER OF BYTES UNTIL DIRECTLY BEFORE Content ID (DATA TO BE FILLED IN BY Mastering Facility) AND START LOCATION OF Content Certificate.
UK_Inf_Location: Physical Sector Number OF TITLE KEY FILE START LOCATION. IF NO Unit_Key.inf STORED IN THAT Layer, SPECIFY 00000000_{16}.
UK_Inf_Offset: NUMBER OF BYTES UNTIL DIRECTLY BEFORE Encrypted Unit Key for CPS Unit #1 and THE START LOCATION OF Unit_Key.inf.
Num_of_UK: NUMBER OF Unit Keys OF ENTIRE Disc (= NUMBER OF CPS Units).
MKB_Location: Physical Sector Number OF MKB START LOCATIONS. IN THE EVENT THAT NO MKB_Cert IS STORED, SPECIFY 00000000_{16}.
N: Logical Sector NUMBER OF Layer i.
Encryption_Flag: Flag FOR WHETHER OR NOT TO ENCRYPT.
Data_Type: Flag SHOWING Type OF Sector.
CPS_Unit_No: CPS Unit Number.
Clip_AV_File_No: CLIP FILE NUMBER. INFORMATION TO BE USED FOR THE PURPOSE OF CHT CREATION.
Last_Sector_of_Clip: FLAG SHOWING LAST Sector OF EACH CLIP (REGARDLESS OF Layer).
Last_Sector_of_Layer: FLAG SHOWING LAST Sector OF EACH CLIP IN EACH Layer.

FIG. 15


450
LICENSING ENTITY
351
MKB / Km
470
ENCRYPTING FACILITY
(DISK PLANT)
430
AUTHORING FACILITY
S271
AUTHORING
332
AUTHORIZED CONTENT
451
SCRAMBLE RULE
S272
SCRAMBLING
S273
ENCRYPTING
452
ENCRYPTED CONTENT
451
SCRAMBLE RULE
INFORMATION RECORDING MEDIUM
452
ENCRYPTED CONTENT
100

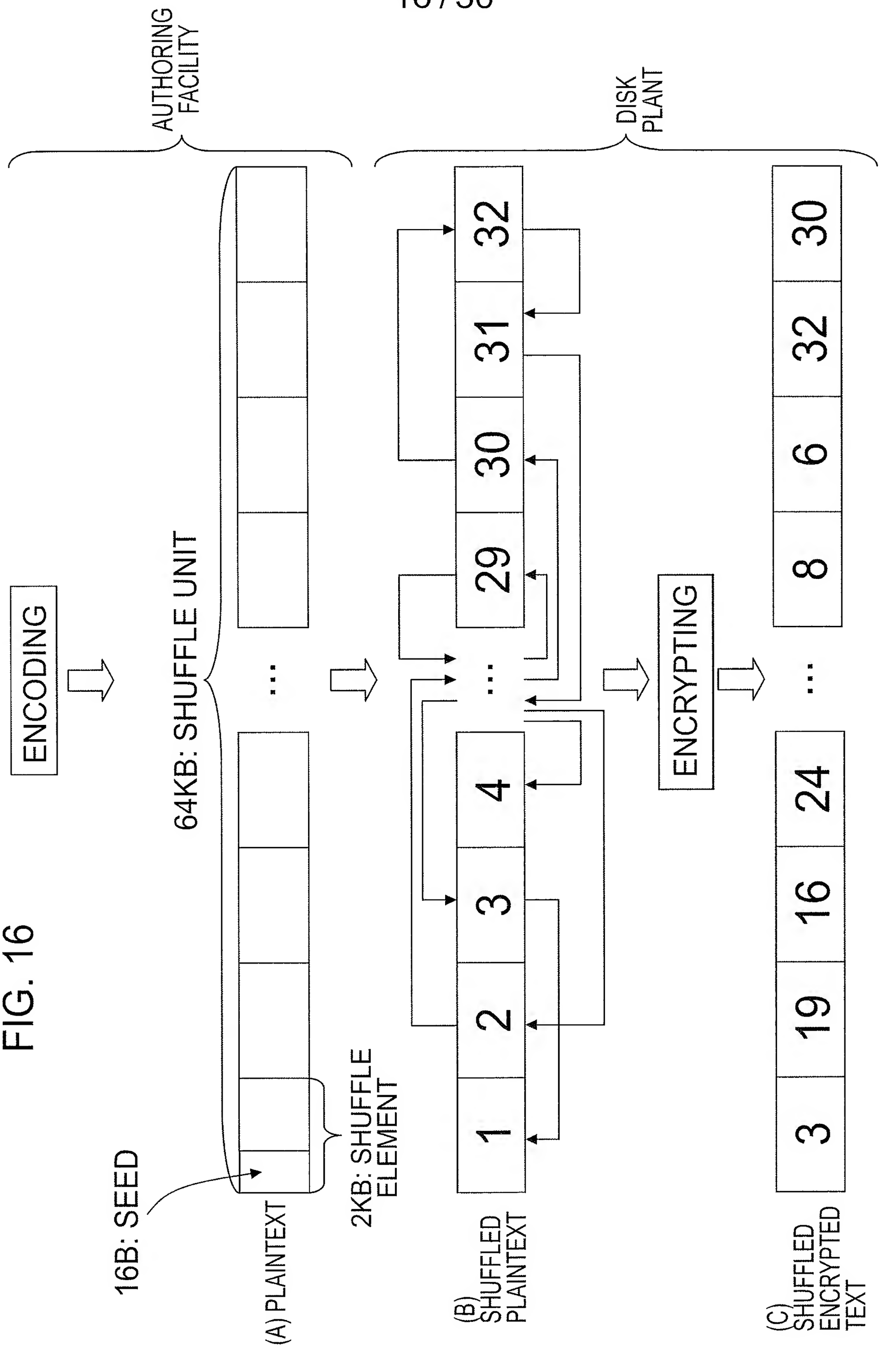

AUTHORING FACILITY
DISK PLANT
ENCODING
64KB: SHUFFLE UNIT
16B: SEED
(A) PLAINTEXT
2KB: SHUFFLE ELEMENT
(B) SHUFFLED PLAINTEXT
ENCRYPTING
(C) SHUFFLED ENCRYPTED TEXT
32
31
30
29
4
3
2
1
30
32
6
8
24
16
19
3

FIG. 16

FIG. 17

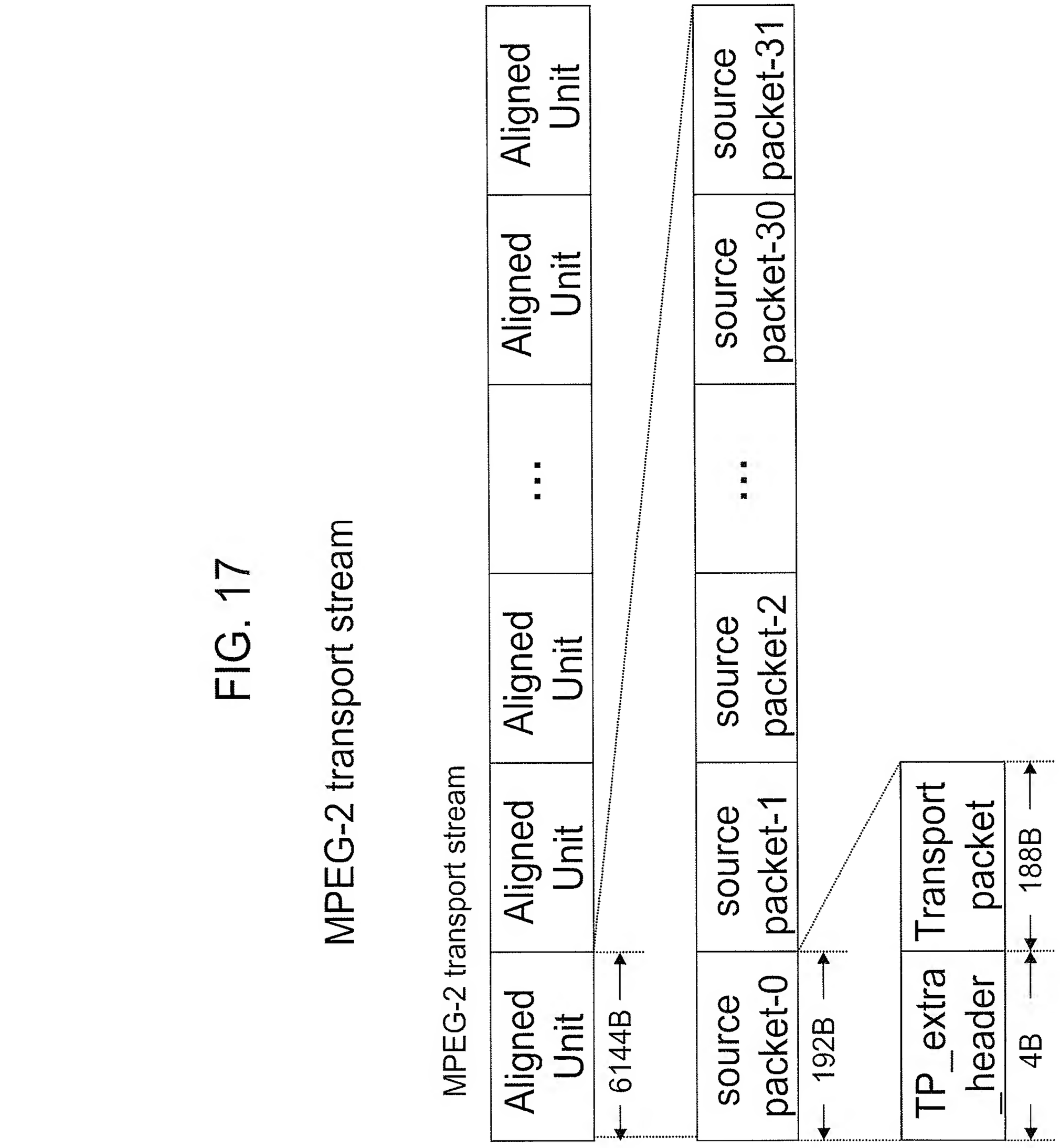

MPEG-2 transport stream
Aligned Unit
...
Aligned Unit
Aligned Unit
source packet-0
source packet-1
source packet-2
source packet-30
source packet-31
6144B
192B
TP_extra header
Transport packet
4B
188B
(A)
(B)
(C)

FIG. 18

(A) SYNTAX OF source_packet

	#bits
source_packet(){	
TP_extra_header()	4
transport_packet()	188
}	

(B) SYNTAX OF TP_extra_header

	#bits
TP_extra_header(){	
is_not_free	1
is_encrypted	1
arrival_time_stamp	30
}	

FIG. 19 SYNTAX OF transport_packet

	#bits
transport_packet(){	
sync_byte	8
transport_error_indicator	1
payload_unit_start_indicator	1
transport_priority	1
PID	13
transport_scrambling_contorl	2
adaptation_field_control	2
continuity_counter	4
if (adaptation_field_control==‘ || adaptation_filed_control==’11’) {	
adaptation field()	
}	
if (adaptation_field_control==‘ || adaptation_filed_control==’11’) {	
adaptation field()	
}	
if (adaptation_field_control==‘ || adaptation_filed_control==’11’) {	
for (i=0; i<N; i++) {	
data_byte	8
}	
}	
}	

FIG. 20

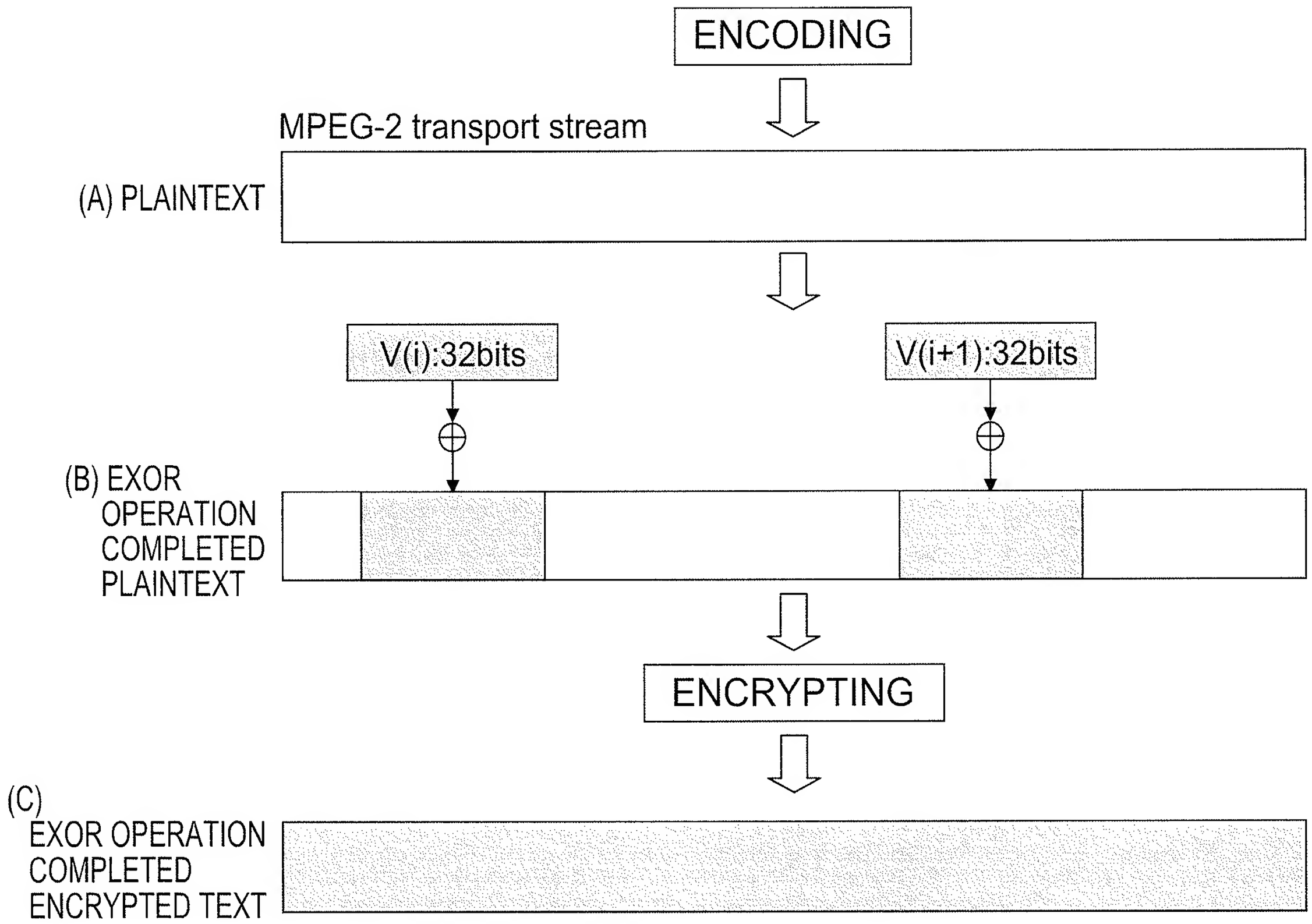
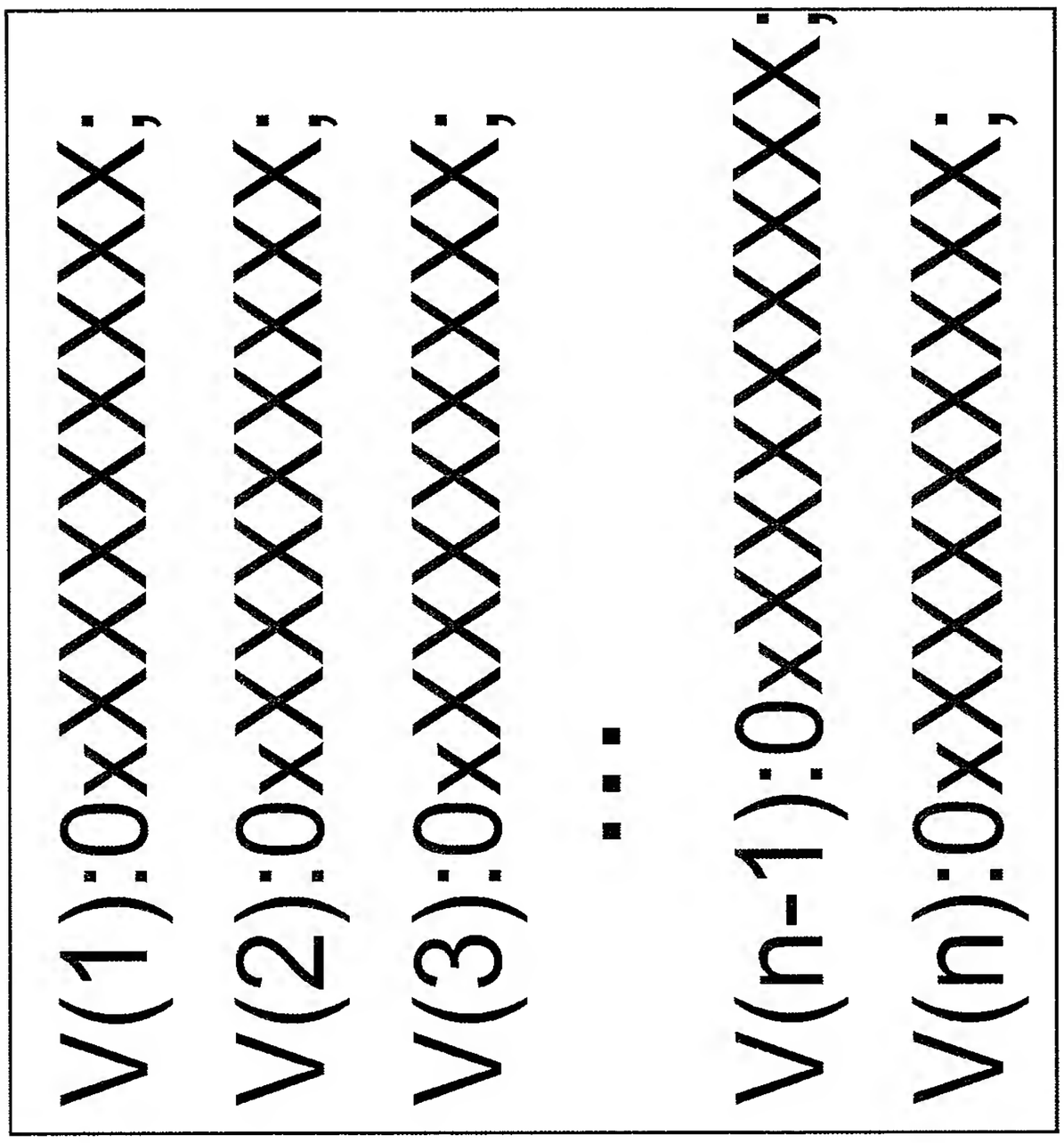

ENCODING
MPEG-2 transport stream
(A) PLAINTEXT
V(i):32bits
V(i+1):32bits
(B) EXOR OPERATION COMPLETED PLAINTEXT
ENCRYPTING
(C) EXOR OPERATION COMPLETED ENCRYPTED TEXT
AUTHORING FACILITY
DISK PLANT

FIG. 21


V(1):0xXXXXXXXX;
V(2):0xXXXXXXXX;
V(3):0xXXXXXXXX;
...
V(n-1):0xXXXXXXXX;
V(n):0xXXXXXXXX;

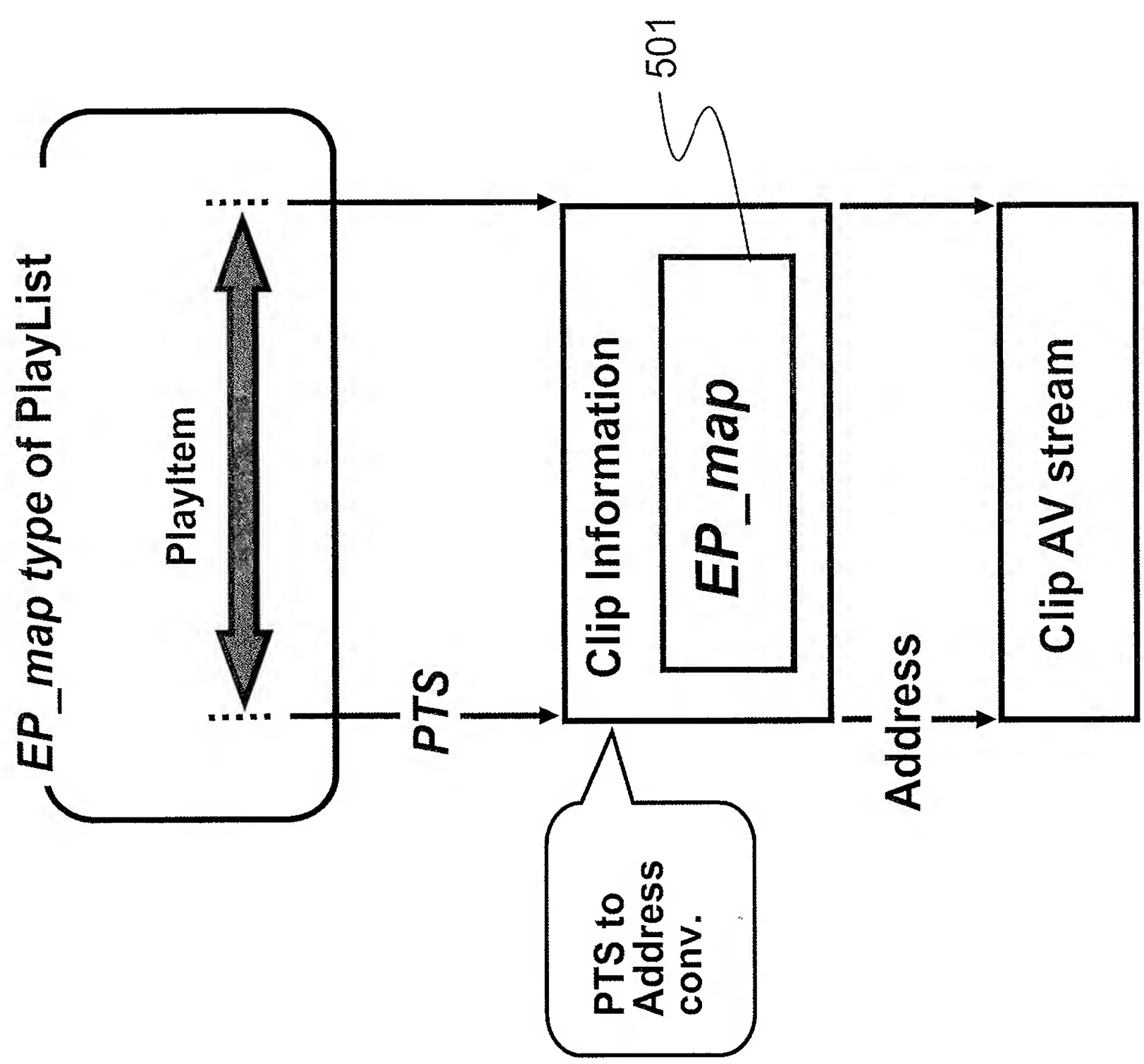

501
EP_map type of PlayList
PlayItem
PTS
Clip Information
EP_map
Address
Clip AV stream
PTS to Address conv.

FIG. 22

FIG. 23

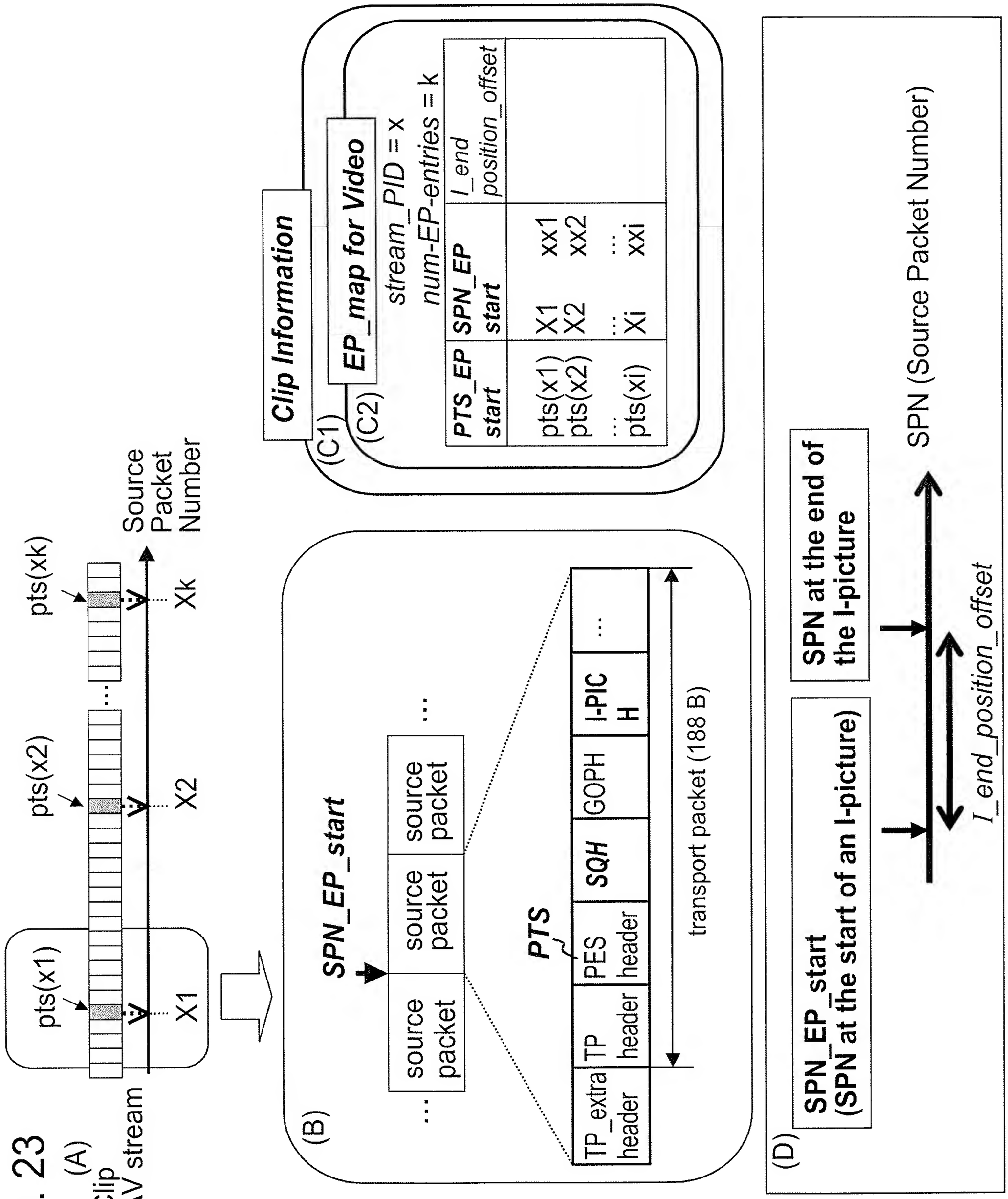
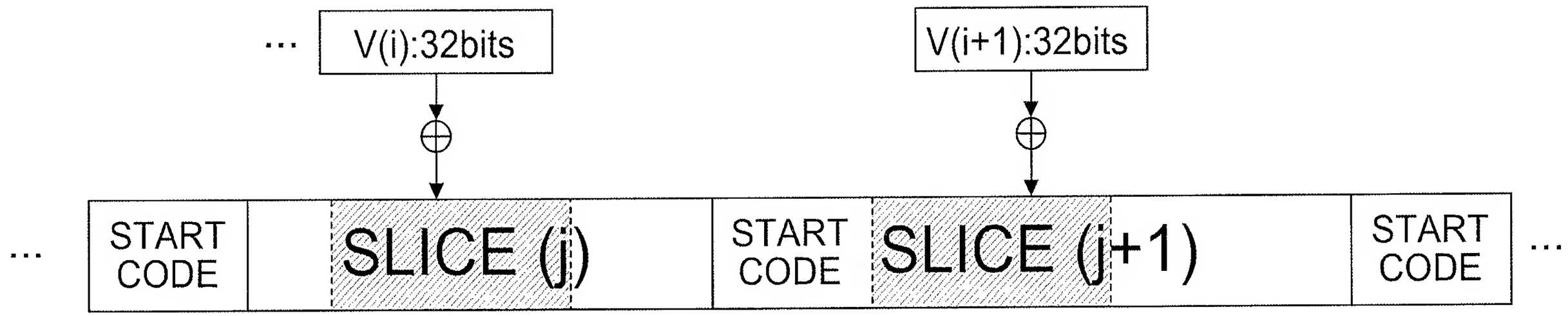
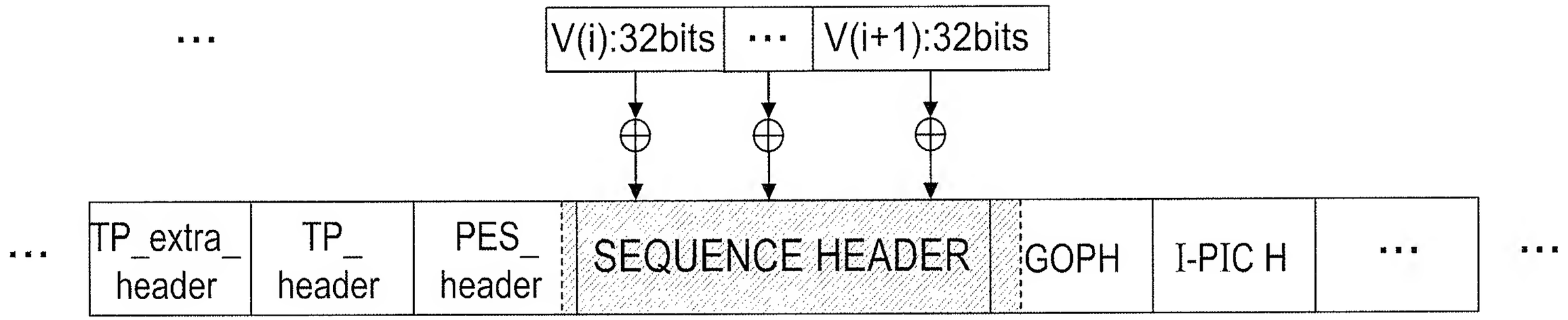

(A)
Clip
AV stream
pts(x1)
pts(x2)
pts(xk)
X1
X2
Xk
Source Packet Number
(B)
SPN_EP_start
source packet
PTS
TP_extra header
TP header
PES header
SQH
GOPH
I-PIC H
transport packet (188 B)
(C1)
Clip Information
(C2)
EP_map for Video
stream_PID = x
num-EP-entries = k
I_end position_offset
PTS_EP start
SPN_EP start
pts(x1) X1 xx1
pts(x2) X2 xx2
pts(xi) Xi xxi
(D)
SPN_EP_start
(SPN at the start of an I-picture)
SPN at the end of the I-picture
SPN (Source Packet Number)
I_end_position_offset

FIG. 24



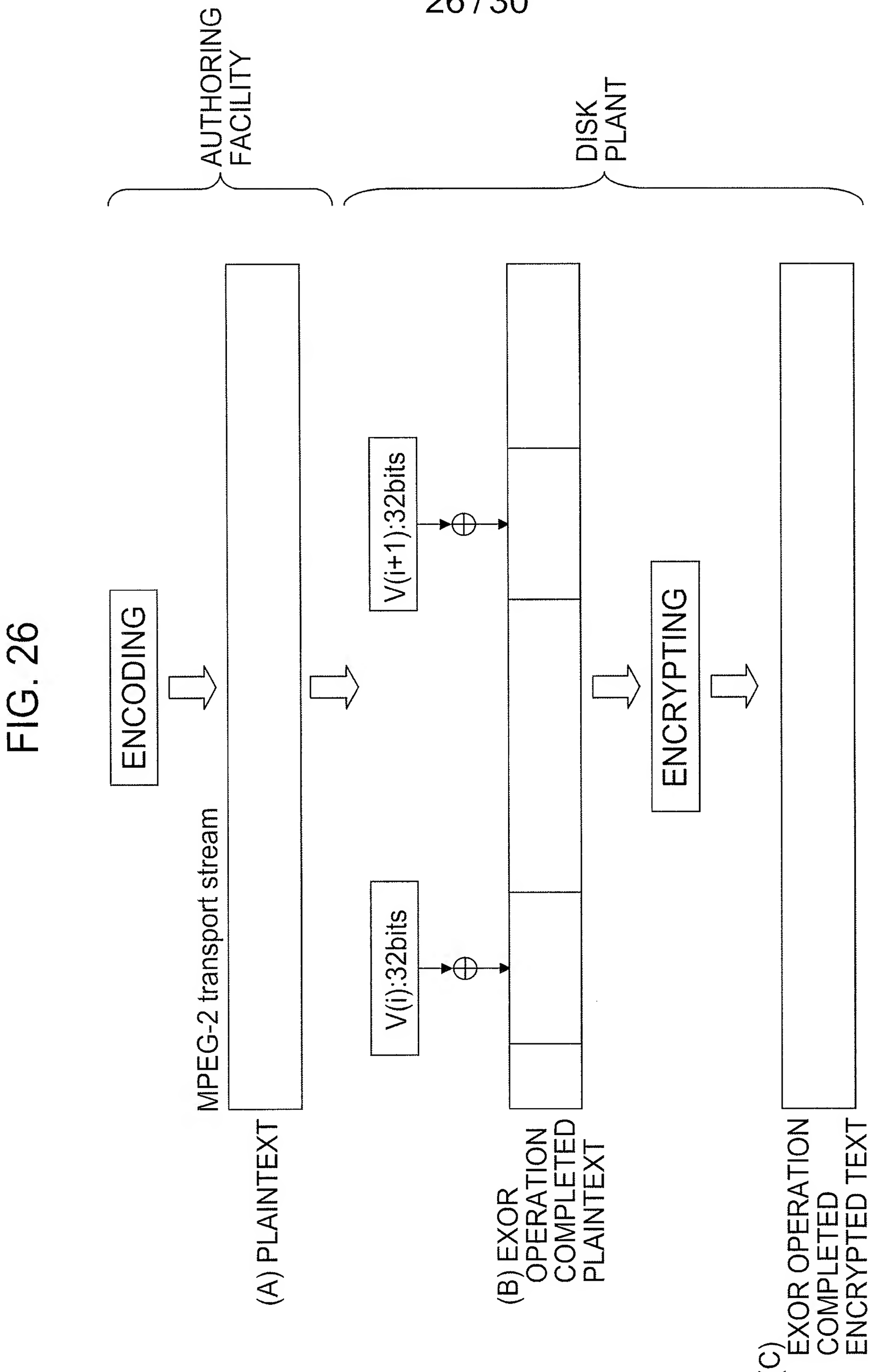
- EACH SLICE IS CODED BY VLC, AND SO BY CHANGING THE VALUE OF A PORTION OF THE CODE THEREOF, THE ENTIRE SLICE CANNOT BE DECODED.
- FURTHER, BY CHANGING THE VALUE OF AN I-PICTURE SLICE, THE ENTIRE CORRESPONDING GOP IS INFLUENCED.
- START CODE: SYNCHRONOUS CODE SHOWING THE HEAD OF THE NEXT SLICE.

FIG. 25



- EACH SEQUENCE HEADER IS A HEADER FOR THE CORRESPONDING GOP, AND BY CHANGING THE VALUE OF ALL PORTIONS OR OF ONE PORTION, THE ENTIRE GOP CANNOT BE DECODED.

FIG. 26


AUTHORING FACILITY
DISK PLANT
ENCODING
MPEG-2 transport stream
(A) PLAINTEXT
V(i):32bits
V(i+1):32bits
(B) EXOR OPERATION COMPLETED PLAINTEXT
ENCRYPTING
(C) EXOR OPERATION COMPLETED ENCRYPTED TEXT

S05P1581

FIG. 27

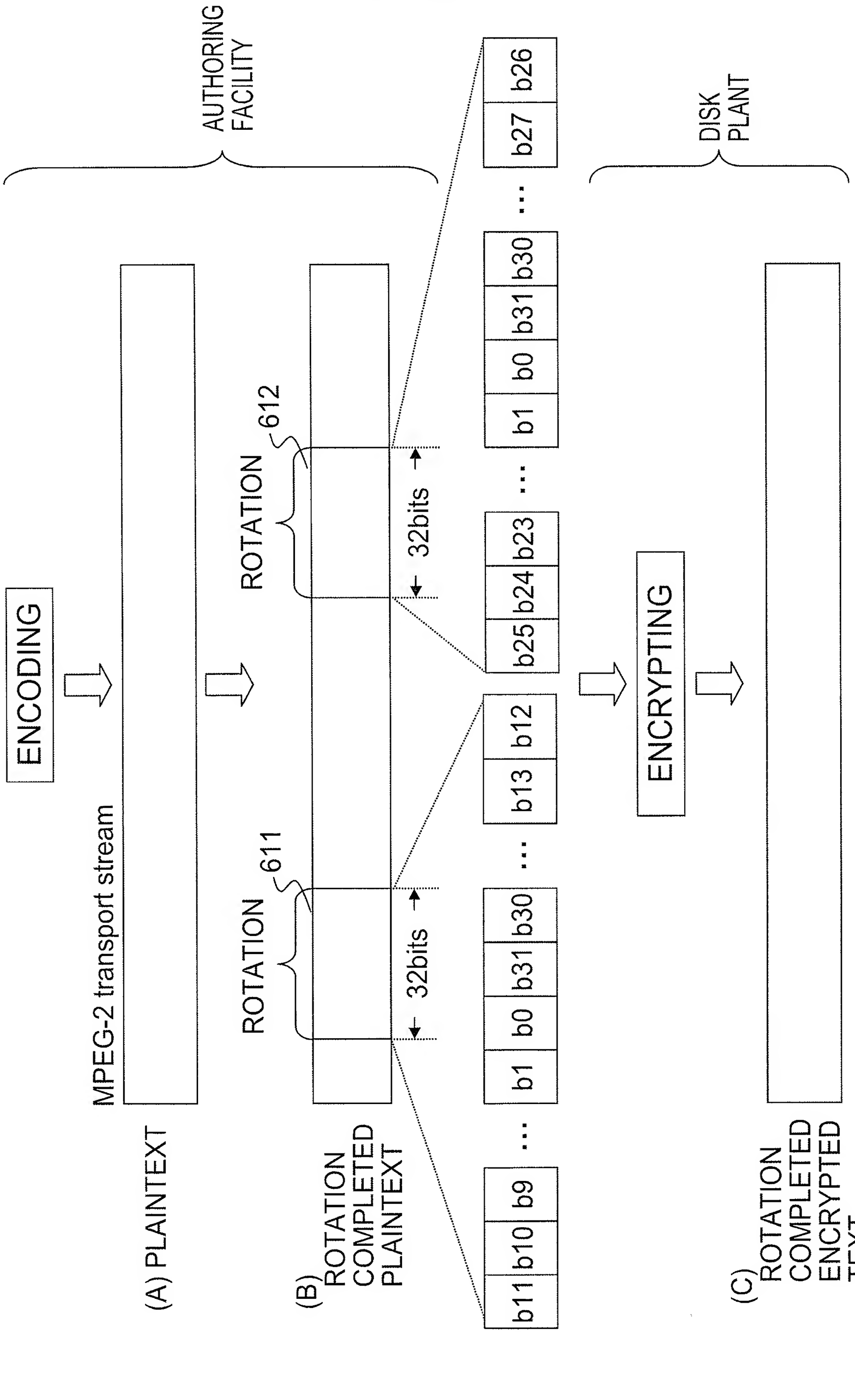


FIG. 28

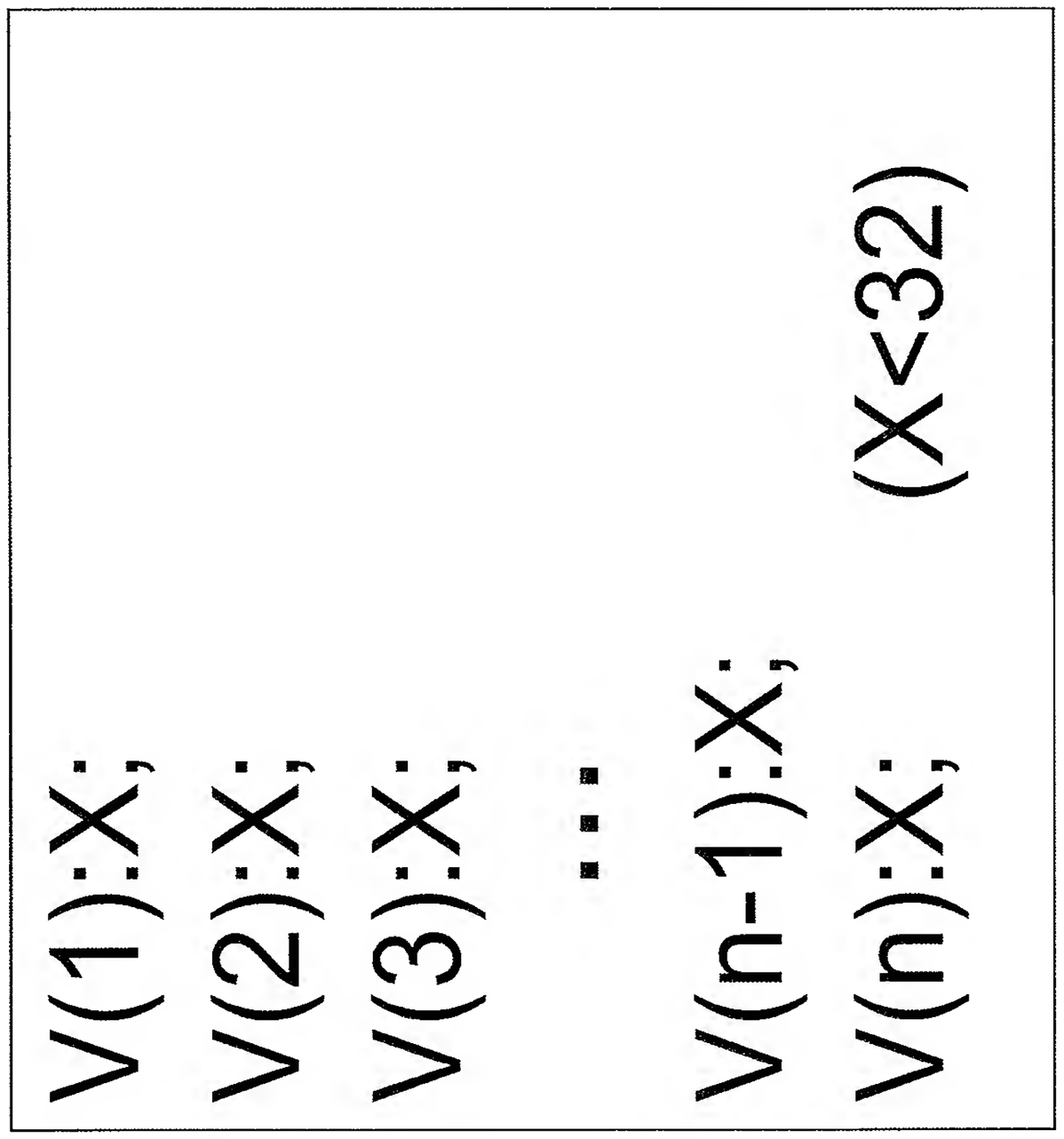
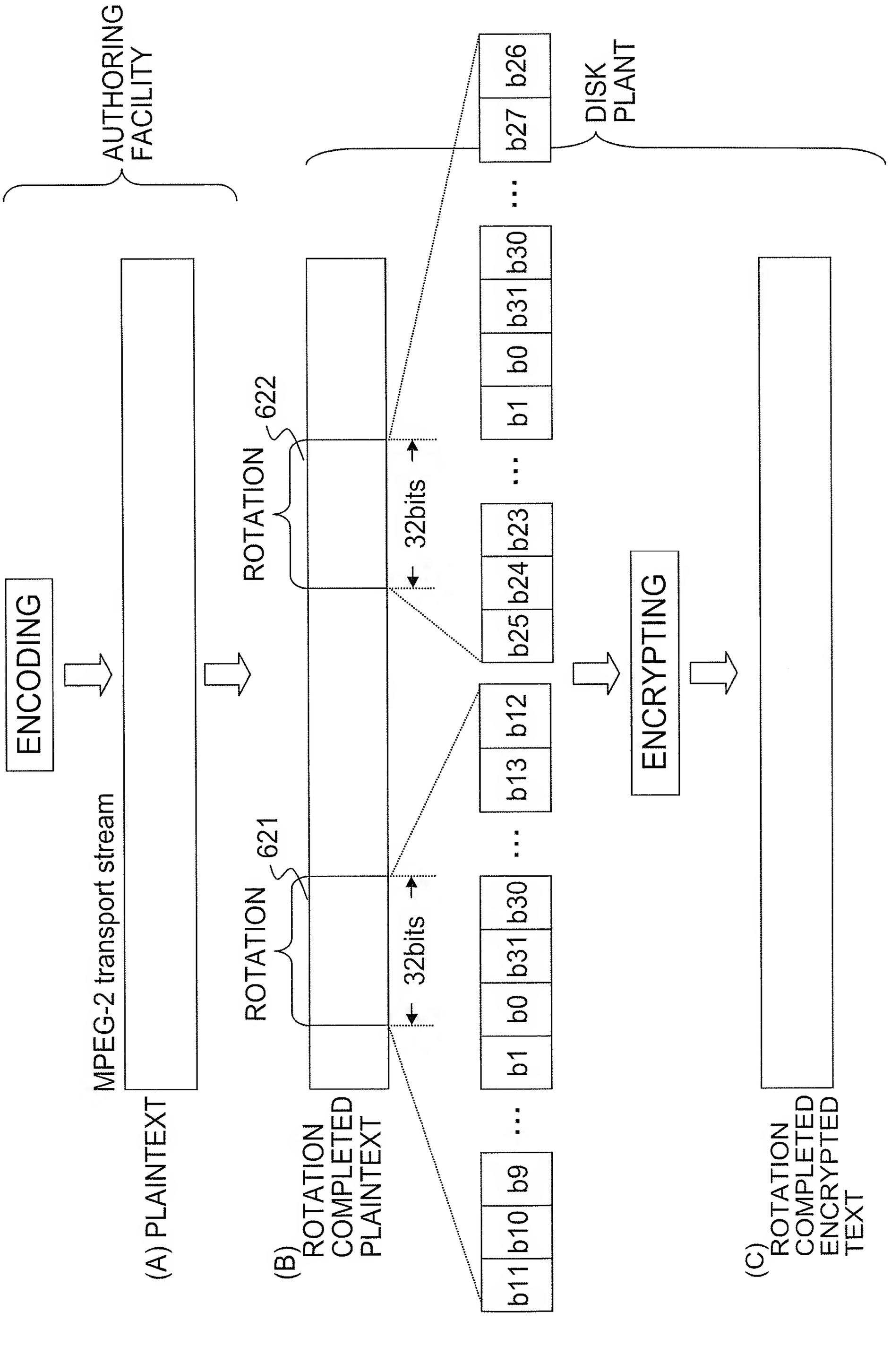


FIG. 29


AUTHORING FACILITY
DISK PLANT
ENCODING
ENCRYPTING
MPEG-2 transport stream
(A) PLAINTEXT
(B) ROTATION COMPLETED PLAINTEXT
(C) ROTATION COMPLETED ENCRYPTED TEXT
ROTATION
622
621
32bits
b0
b1
b9
b10
b11
b12
b13
b23
b24
b25
b26
b27
b30
b31

S05P1581

FIG. 30